REMARKS

Status of claims

Upon entry of the present amendment, claims 1-14 and 17-22 will be pending. Claims 1, 13 and 17 will have been amended. Reconsideration of the Office Action of February 10, 2009 is respectfully requested.

I. Rejection under 35 U.S.C. § 102

The Examiner rejected claims 1-14 and 17-22 under 35 U.S.C. 102(b) as being anticipated by Van Oorshot et al., U.S. Patent Number 6,229,894. The Examiner continues to assert that Van Oorshot et al. teach the limitations of claims 1-14 and 17-22. With regard to claim 1, the Examiner asserted that Van Oorshot et al. teach a method for monitoring (column 2, lines 4-10 indicate the needs of the law enforcement agencies in the monitoring of communications) of communications traffic, comprising: recording packet-data communication traffic received from, and passing through, a network switch, encrypting the packet-data communication traffic after the packet-data communication traffic has passed through the network switch to create encrypted data (column 5, lines 56-65; and encrypted transmission (ciphertext) 54 in Figure 2 which includes the signature of sending end-user 56, the encrypted file or message 58, and the wrapped session key 52, and storing of communications data as well as a decryption key required for its decoding) such that the encrypted data can be decrypted only by means of decryption keys that exhibit restricted availability (column 4 line 59 to column 5, line 5).

As to claim 17, the Examiner asserted Van Oorshot et al. teach "'a method for monitoring of communications traffic, comprising the steps of:" "receiving communications traffic from a network switch;" "encrypting the communications traffic after the packet-data communication traffic has passed through the network switch (Van Oorshot: column 5, lines 56-65 - also see encrypted transmission (ciphertext) 54 in Figure 2 which includes the signature of sending end user 56, the encrypted file or message 58, and the wrapped session key 52) to generate encrypted

communications traffic data (Van Oorshot: Figure 1, and its description starting in column 3, line 15 discloses the receiving, encrypting, recording, and storing of communications data as well as a decryption key required for its decoding);" "recording the encrypted communications traffic data (see server 16, processing device 90, memory 92 of Figure 2, and column 7, lines 17-27);" "storing the recorded encrypted communications traffic data such that the encrypted communications traffic data can be decrypted by decryption keys that exhibit restricted availability, that allow encrypted search conditions and that employ separate levels of authorization for access to the stored data (see secure storage of users' decryption private keys of server 16 in Figure 2, and column 7, lines 27-30; and directory 68 (a database) of Figure 2, and column 6, lines 50-54); and "encrypting details relating to the communications traffic and storing the said encrypted details for subsequent access (see sending end-user 18, and end-user encryption certificate of end-user 60, 62, 64 in Figure 2, and column 5, lines 39-55)."' Applicant respectfully traverses.

In sustaining the rejection under 35 U.S.C. § 102(b), the Examiner is failing to adhere to MPEP 2131, which states in bold capitals the following "**TO ANTICIPATE A CLAIM, THE REFERENCE MUST TEACH EVERY ELEMENT OF THE CLAIM**" (emphasis in original). Van Oorshot et al. do not teach explicitly recited elements of claims 1, 13 and 17 – even before the amendment to these claims presented herein. Claims 1, 13 and 17 each recite that the packet-data communication traffic is encrypted *after* it passes through a network switch. In contrast, Van Oorshot et al. do not teach or suggest a encrypting the communication traffic *after it has passed through the network switch*. Rather, Van Oorshot et al. teach user-level encryption of data, where the data is encrypted on a user device prior to transmission ("each of the end-users are equipped with at least one symmetric encryption algorithm, such as DES, and has an asymmetric public/private key pair and an asymmetric (public key) algorithm. As such, when an end-user is transmitting secured data to a receiving party, the sending party encrypts a symmetric key using the public encryption key of 45 the receiving party, or recipient end-user." See, col. 3, lines 40-45 and additional like description at col. 5, line 30 – col. 6, line 10). Figure 2 of Van Oorshot et al. further illustrates that encryption is performed by end-users 18-22 before

the communication is transmitted from the end-user device (see data 50 as it flows into the box "sending end-user 18" and flows out as encrypted transmission (ciphertext) 54). Therefore, Applicant submits that sustaining a rejection under 35 U.S.C. § 102(b) is improper, as each and every element of the claims is not taught in Van Oorshot et al.

Applicant has amended claims 1, 13 and 17 (although not for reasons related to patentability, as noted above) to further clarify which elements disclosed in the instant specification are performing the recited processes in the claims.

With regard to claims 2-12, 14 and 18-22, Applicant notes that these claims depend from what is believed to be an allowable base claim (i.e., claims 1, 13 and 17, respectively). As such, without addressing the propriety of the Examiner's rejection. Applicant submits that claims 2-12, 14 and 18-22 are now allowable over the prior art of record.

In view of the above, the Examiner is respectfully requested to reconsider and withdraw the rejection of claims 1-14 and 17-22 under 35 U.S.C. 102(b) as being anticipated by Van Oorshot et al.

CONCLUSION

Applicants respectfully assert that all of the pending claims are allowable over the references of record, and requests entry of a Notice of Allowance.

Respectfully submitted,

Date: May 8, 2009

/Lawrence A. Aaronson/
Lawrence A. Aaronson
Reg. No. 38,369

Lawrence A. Aaronson, P.C.
12850 Highway 9
Suite 600 - PMB 338
Alpharetta, GA 30004
Telephone: (770) 475-9129
Facsimile: (770) 809-5028